UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/598,719 | 09/08/2006 | Agostinho De Arruda Villela | 2171323-000002 | 9289 |

44777 7590 09/18/2008
W. EDWARD RAMAGE
COMMERCE CENTER SUITE 1000
211 COMMERCE ST
NASHVILLE, TN 37201

| EXAMINER | |
|---|---|
| WRIGHT, BRYAN F | |
| ART UNIT | PAPER NUMBER |
| 2131 | |
| MAIL DATE | DELIVERY MODE |
| 09/18/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

|  |  |  |  |
|---|---|---|---|
| ***Office Action Summary*** | **Application No.**<br>10/598,719 | **Applicant(s)**<br>DE ARRUDA VILLELA, AGOSTINHO | |
|  | **Examiner**<br>BRYAN WRIGHT | **Art Unit**<br>2131 | |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *08 September 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *17-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *17-35* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 September 2006* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *1/22/2007*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

## DETAILED ACTION

1. This action in response to application September 8, 2006. Claims (17-35) are pending.

## Priority

2. Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) - (d) is acknowledged.

The application is filed on September 8, 2006 but is a 371 case of PCT/BR05/00030 application filed 03/10/2005 and has a foreign priority application BRAZIL Plo100265-2 filed on 03/10/2004.

## *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claim 31 rejected under 35 U.S.C. 102(b) as being anticipated by Schwartz et al (US Patent Publication No. 20010044896 and Schwartz hereinafter).

4. As to claim 31, Schwartz teaches **a method for identifying devices and controlling access to a service, comprising the steps of: registering a device with an authentication server for access to the service** [fig. 3]; **and verifying the identity of the device each time it subsequently attempts to access the service** (i.e., .. teaches an device signature verification [fig. 4; par. 84]).

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 32-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schwartz in view of Cui et al. (US Patent Publication No. 2005/0166053 and Cui hereinafter).

**6.** As to claim 32, Schwartz teaches a **method where the step of registering a device comprises the steps of:**

**and sending the digital signature of the device to an authentication server** (for purposes of signature authentication Schwartz provides the capability to send a device signature to a server for authentication [fig. 4]).

**verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero** [par. 102]**;**

However Schwartz does not teach:

**a software agent installed on a device, adapted to collect data related to software and hardware configuration of the device**;

**a digital signature for the device, generated by the software agent by hashing the software and hardware configuration data**;

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Schwartz as introduced by Cui. Cui discloses:

**a software agent installed on a device, adapted to collect data related to software and hardware configuration of the device** (for purposes of collecting data Cui provides a user agent (UA) executing on the mobile device configured to receive information, including but not limited to, at least one device signature, cookie, content for display and the like, a Uniform Resource Locator (URL) [par. 28]);

**a digital signature for the device, generated by the software agent by hashing the software and hardware configuration data (**for purpose of generating a digital signature Cui provides capability to generated a digital signature utilizing a hash function [claim 12[);

Therefore, given the teachings of Cui, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Schwartz by employing the well known features of creating a digital signature utilizing a hash function and software agent disclosed above by Cui, for which digital signature generation will be enhanced [claim 12].

7. As to claim 33, Schwartz teaches a **method where the step of verifying the identity of the device comprises the steps of:**

**and sending the digital signature of the device to an authentication server** (i.e., ... teaches send a device signature to a server for authentication [fig. 4]).

**and comparing the digital signature sent with one or more previously-stored digital signatures for the device** [par. 78]**;**

However Schwartz does not teach:

**a software agent installed on a device, adapted to collect data related to software and hardware configuration of the device**;

**a digital signature for the device, generated by the software agent by hashing the software and hardware configuration data**;

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Schwartz as introduced by Cui. Cui discloses:

**a software agent installed on a device, adapted to collect data related to software and hardware configuration of the device** (for purposes of collecting data Cui provides a user agent (UA) executing on the mobile device configured to receive information, including but not limited to, at least one device signature, cookie, content for display and the like, a Uniform Resource Locator (URL) [par. 28]);

**a digital signature for the device, generated by the software agent by hashing the software and hardware configuration data** (for purpose of generating a digital signature Cui provides capability to generated a digital signature utilizing a hash function [claim 12[);

Therefore, given the teachings of Cui, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Schwartz by employing the well known features of creating a digital signature utilizing a hash function and software agent disclosed above by Cui, for which digital signature generation will be enhanced [claim 12].

**8.** As to claim 34, Schwartz teaches a **method where the step of verifying the identity of the device comprises the steps of:**

**and sending the digital signature of the device to an authentication server** (for purposes of signature authentication Schwartz provides the capability to send a device signature to a server for authentication [fig. 4]).

**and verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero** [par. 102]**;**

However Schwartz does not teach:

**a software agent installed on a device, adapted to collect data related to software and hardware configuration of the device**;

**a digital signature for the device, generated by the software agent by hashing the software and hardware configuration data**;

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Schwartz as introduced by Cui. Cui discloses:

**a software agent installed on a device, adapted to collect data related to software and hardware configuration of the device** (for purposes of collecting data Cui provides a user agent (UA) executing on the mobile device configured to receive information, including but not limited to, at least one device signature, cookie, content for display and the like, a Uniform Resource Locator (URL) [par. 28]);

**a digital signature for the device, generated by the software agent by hashing the software and hardware configuration data** (for purpose of generating a digital signature Cui provides capability to generated a digital signature utilizing a hash function [claim 12]);

Therefore, given the teachings of Cui, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Schwartz by employing the well known features of creating a digital signature utilizing a hash function and software agent disclosed above by Cui, for which digital signature generation will be enhanced [claim 12].

**9.** As to claim 35, Schwartz teaches a **system for identifying devices and controlling access to a service, comprising the steps of:**

**and sending the digital signature of the device to an authentication server** (i.e., teaches send a device signature to a server for authentication [fig. 4]).

**and verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero** (i.e.., .. teaches a determination is made as to the lack of agreement of the device signature and device key stored in the database [par. 102])**;**

**and an authentication server that determines whether the device can access the service based upon the digital signature of the device** [fig. 4].

However Schwartz does not teach:

**a software agent installed on a device, adapted to collect data related to software and hardware configuration of the device**;

**a digital signature for the device, generated by the software agent by hashing the software and hardware configuration data**;

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Schwartz as introduced by Cui. Cui discloses:

**a software agent installed on a device, adapted to collect data related to software and hardware configuration of the device** (for purposes of collecting data Cui provides a user agent (UA) executing on the mobile device configured to receive information, including but not limited to, at least one device signature, cookie, content for display and the like, a Uniform Resource Locator (URL) [par. 28]);

**a digital signature for the device, generated by the software agent by hashing the software and hardware configuration data** (for purpose of generating a digital signature Cui provides capability to generated a digital signature utilizing a hash function [claim 12[);

Therefore, given the teachings of Cui, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Schwartz by employing the well known features of creating a digital signature utilizing a hash function and software agent disclosed above by Cui, for which digital signature generation will be enhanced [claim 12].

10. Claims 17-23, 26 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cui in view of Schwartz.

**11.** As to claim 17, Cui teaches a **method for identifying devices and controlling access to a service, comprising the steps of:**

**collecting data related to software and hardware configurations from a device through a software agent** (i.e., teaches a mobile computing device is configured to provide to a server information associated with a user agent that may be executing on it [par. 16] ... further teaches a client may be configured to enable the sending of information associated with the at least one user agent, mobile device 102, and the like, as well as to receive information, including but not limited to, at least one device signature, cookie, content for display and the like, a Uniform Resource Locator (URL) [par. 28]);

**generating a digital signature for the device by hashing the software and hardware configuration data;** (i.e., ... teaches a subid, gatewaygrp, UA, and a time stamp are hashed to generate a tier 1 device signature [par. 62]; par. 65]).

However Cui does not teach:

**and sending the digital signature of the device to an authentication server**.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Cui as introduced by Schwartz. Schwartz discloses:

**and sending the digital signature of the device to an authentication server** (for purposes of signature authentication Schwartz provides the capability to send a device signature to a server for authentication [fig. 4]).

Therefore, given the teachings of Schwartz, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Cui by employing the well known features of authenticating a device digital signature disclosed above by Schwartz, for which electronic transactions will be enhanced [fig. 4].

12. As to claims 18, the system disclosed by Cui shows substantial features of the claimed invention (discussed in the paragraphs above), it fails to disclose:

A **method where the digital signature sent to the authentication server is encrypted** [claim 18].

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Cui as introduced by Schwartz. Schwartz discloses:

A **method where the digital signature sent to the authentication server is encrypted** [claim 18] (for purposes of encrypting the digital signature Schwartz provides the encryption capability [par. 109].

Therefore, given the teachings of Schwartz, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Cui by employing the well known features of encrypting a digital signatures disclosed above by Schwartz, for which digital signature transmission for electronic transactions will be enhanced [par. 109].

13. As to claim 19, Cui teaches a **method where the software agent is installed on the device as part of the process of using the device to access a service** (i.e., ... teaches a associated information may further include information about the user agent (UA) executing on the mobile device [par. 53]).

14. As to claim 20, Cui teaches a **method where the hashes used to generate the digital signature are changed with every attempt to access a service, and the hashes cannot be reversed** (i.e., .. teaches a one-way hash function [par. 63] ... further teaches updating (rolling) the device signature(s) is based, in part, on a pre-determined period of time [par. 70]).

15. As to claim 21, Cui teaches a **method where the digital signature is one of several stages of a framework of authorization and authentication processes governing access to the service by the device** [fig, 3].

16. As to claims 22, 26, and 27, the system disclosed by Cui shows substantial features of the claimed invention (discussed in the paragraphs above), it fails to disclose:

> **A method where the authentication server compares the digital signature sent with one or more previously-stored digital signatures** (claim 22).
>
> **A method where the authentication server allows minor modifications to the software or hardware configurations of a previously- enrolled device so as to preserve access or denial of access for the device** (claim 26).
>
> **A method where the previously-stored digital signature of the device is updated to reflect the modifications** (claim 27).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Cui as introduced by Schwartz. Schwartz discloses:

> **A method where the authentication server compares the digital signature sent with one or more previously-stored digital signatures** (claim 22) (for purposes of authentication Schwartz provides the capability to compare digital signatures [par. 102]).

**A method where the authentication server allows minor modifications to the software or hardware configurations of a previously- enrolled device so as to preserve access or denial of access for the device** (claim 26) (for purposes of authentication Schwartz provide a control policy for which allows modification to configuration within authentication guidelines [par. 94]).

**A method where the previously-stored digital signature of the device is updated to reflect the modifications** (claim 27) (for purpose of modifying previous stored digital signature Schwartz provides the capability to invalidate previously stored signature and invalidate previously stored signature with new signatures [par. 78].

Therefore, given the teachings of Schwartz, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Cui by employing the well known features of a configuration control policy and signature modification disclosed above by Schwartz, for which device access to services will be enhanced [par. 94].

17. As to claims 23, the system disclosed by Cui shows substantial features of the claimed invention (discussed in the paragraphs above), it fails to disclose:

> **A method where the authentication server determines whether the device has been excluded from accessing or enrolling in the service by determining whether the device is on a list or in a group of devices not allowed to access the service, or is included within a group of devices allowed to access the service** [claim 23].

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Cui as introduced by Schwartz. Schwartz discloses:

> **A method where the authentication server determines whether the device has been excluded from accessing or enrolling in the service by determining whether the device is on a list or in a group of devices not allowed to access the service, or is included within a group of devices allowed to access the service** [claim 23] (for purposes of authentication Schwartz provides the capability to authenticate a device on the base of access criteria stored in database [par. 88]).

Therefore, given the teachings of Schwartz, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Cui by employing the well known features of maintaining authentication access criteria and performing authentication based on criteria disclosed above by Schwartz, for which electronic transactions will be enhanced [par. 88].

18. Claims 24, 25, 29 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cui in view of Schwartz as applied to claims 17 and 22 above, and further in view of Matsuzaki et al. (WO 2004023275 and Matsuzaki hereinafter).

19. As to claims 24, 25, 29 and 30, the system disclosed by Cui in view of Schwartz shows substantial features of the claimed invention (discussed in the paragraphs above), it fails to disclose:

**A method where the authentication server allows a maximum number of enrollments for a particular device** (claim 24).

**A method where the maximum number of enrollments is zero** (claim 25).

**A method where multiple devices can be registered for a single user with the authentication server to create a registration hierarchy** (claim 29).

**A method where a user can unregister a device only through the device itself, or another device within the registration hierarchy registered earlier than the device to be unregistered** (claim 30).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Cui in view of Schwartz as introduced by Matsuzaki. Matsuzaki discloses:

> **A method where the authentication server allows a maximum number of enrollments for a particular device** (claim 24) (for purposes of allowing a maximum number of device enrolled device Matsuzaki provides the capability to limit the number of devices enrolled [abstract]).
>
> A **method where the maximum number of enrollments is zero** (claim 25) for purposes of allowing a maximum number of device enrolled device Matsuzaki provides the capability to limit the number of devices enrolled [abstract]).
>
> **A method where multiple devices can be registered for a single user with the authentication server to create a registration hierarchy** (claim 29) (for purposes of a registration hierarchy Matsuzaki provides registration hierarchy for registering devices [fig. 16].
>
> **A method where a user can unregister a device only through the device itself, or another device within the registration hierarchy registered earlier than the device to be unregistered** (claim 30) (for purpose of unregistering a device Matsuzaki provides decision capability to determine device status according to registration information [pg. 19, lines 10-25].

Therefore, given the teachings of Matsuzaki, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Cui in view of Schwartz by employing the well known features of device registration disclosed above by Matsuzaki, for which controlling access to services will be enhanced [abstract].

20. Claim 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cui in view of Schwartz as applied to claim 17 above, and further in view of Wade et al. (US Patent No. 5,552,776 and Wade hereinafter).

21. As to claim 28, the system disclosed by Cui in view of Schwartz shows substantial features of the claimed invention (discussed in the paragraphs above), it fails to disclose:

> **A method where the authentication server logs all accesses or attempted accesses by a device to the service (**claim 28)

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Cui in view of Schwartz as introduced by Wade. Wade discloses:

**A method where the authentication server logs all accesses or attempted accesses by a device to the service (**claim 28) (for purposes of logging access attempts Wade provides the capability login attempts [col. 9, lines 15-25]).

Therefore, given the teachings of Wades, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Cui in view of Schwartz by employing the well known features of limiting the number of enrolled devices disclosed above by Wades, for which controlling access to services will be enhanced [abstract].

## Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2131

/Christopher A. Revak/
Primary Examiner, Art Unit 2131